

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

v.

DECISION AND ORDER
10-CR-110A

JEFF COON,

Defendant.

INTRODUCTION

Defendant Jeff Coon is charged with one count of distribution of child pornography, one count of receipt of child pornography, and three counts of possession of child pornography. On June 21, 2010, the defendant filed a motion to suppress evidence seized pursuant to a search warrant issued by Magistrate Judge Hugh B. Scott on March 31, 2009. The motion to suppress was referred to Magistrate Judge Scott, pursuant to 28 U.S.C. § 636. On August 20, 2010, Magistrate Judge Scott issued a Report and Recommendation ("Initial Report and Recommendation") wherein he found that probable cause to issue the warrant was lacking. The government moved for reconsideration of the Initial Report and Recommendation and on November 8, 2010, Magistrate Judge Scott issued a second Report and Recommendation ("Second Report and Recommendation"). The Second Report and Recommendation reversed his Initial Report and Recommendation and found, instead, that there was probable cause to issue the search warrant.

The defendant filed objections to the Second Report and Recommendation and

the government filed a response. In his objections, the defendant argues that: (1) it was improper for the Magistrate Judge to reconsider his Initial Report and Recommendation; and (2) the Magistrate Judge's recommendation to deny suppression is erroneous. In response, the government argues that the Magistrate Judge had authority to reconsider and reverse his Initial Report and Recommendation and correctly found, in the Second Report and Recommendation, that there existed probable cause to issue the warrant. Alternatively, the government asserts that the good faith exception to the warrant requirement applies.¹

On April 11, 2011, this Court heard oral argument on the defendant's objections and requested additional briefing. The matter was deemed submitted on April 15, 2011. For the reasons stated, the Court finds that (1) probable cause to issue the warrant was lacking, but (2) the good faith exception applies. Accordingly, the motion to suppress is denied.

BACKGROUND

On April 11, 2008, a Federal German Police (Bundeskriminalamt or "BKA") computer crime unit downloaded from the IP address 71.186.130.148, a video depicting child pornography. On May 6, 2008, the BKA requested assistance from the United States Immigration and Customs Enforcement (ICE) Cyber Crimes Center to identify the subscriber of the IP address on April 11, 2008 - the date that the video was downloaded. In that notice, German Police identified Verizon as the IP address holder.

¹ The Magistrate Judge did not reach the issue of good faith.

On February 25, 2009, almost ten months after being notified by the BKA, ICE issued a summons to Verizon requesting the subscriber name associated with IP address 71.186.130.148 on the date in question --April 11, 2008. The following day, Verizon complied, identifying Tabitha Coon, located at 422 21st Street in Niagara Falls, New York, as the user of IP address 71.186.130.148 on April 11, 2008. Verizon's response also advised that the Coon account was opened in February 2008 and closed in August 2008.

At some point thereafter, ICE conducted public records and utility checks and determined that Tabitha and Jeff Coon resided at 422 21st Street in Niagara Falls, New York. On March 31, 2009, ICE agents presented this information to Magistrate Judge Scott and requested a warrant to search 422 21st Street, Niagara Falls, New York. In the warrant application, agents advised the Magistrate Judge that: (1) they had learned from German authorities that an individual with the IP address of 71.186.130.148 had downloaded a video containing child pornography on April 11, 2008; (2) in response to a subpoena, Verizon identified the subscriber using that IP address on that date as Tabitha Coon at 422 21st Street, Niagara Falls; and (3) that a public records and utility check of that residence revealed that, as of March 20, 2009, Tabitha and Jeff Coon reside at that location. The warrant did not indicate that the Coon's Verizon account had closed in August 2008.

Magistrate Judge Scott issued the warrant on March 31, 2009. The warrant was executed on April 6, 2009, almost a full year after the child pornography had been discovered by the BKA. Agents seized multiple computers, hard drives and storage media from the defendant's residence. Forensic analysis of that computer uncovered

several images of child pornography. As noted, a six-count indictment was filed against the defendant on April 15, 2010.

DISCUSSION

The defendant moves to suppress the evidence seized arguing that probable cause was lacking. He contends that the information in the warrant application was simply too stale to provide probable cause as almost an entire year had elapsed between the time the child pornography was first discovered by the BKA (April 11, 2008) and the time that the warrant was ultimately executed (April 6, 2009).

In response, the government points out that technology exists to recover deleted computer files. Because forensic experts can recover computer evidence long after files have been deleted, the government asserts that there was a “fair probability” that the downloaded child pornography would still be on the defendant’s computer.

Before addressing the merits of the staleness argument, the Court rejects the defendant’s contention that the Magistrate Judge lacked authority to reconsider his Initial Report and Recommendation. Like district judges, magistrate judges possess the inherent authority to reconsider their own interlocutory orders prior to the entry of judgment. *See United States v. LoRusso*, 695 F.2d 45 (2d Cir. 1982)(“A district court has the inherent power to reconsider and modify its interlocutory orders prior to the entry of judgment.”); *see also United States v. Green*, 414 F.2d 1174, 1175 (D.C.Cir.1969) (trial judge had authority to withdraw oral decision granting defendant's motion to dismiss indictment); *United States v. Jerry*, 487 F.2d 600, 604-05 (3d

Cir.1973) (district court had authority to rescind written order improvidently permitting defendant to withdraw guilty plea). In any event, the Magistrate Judge's authority to revoke or reverse his Initial Report and Recommendation is irrelevant because this Court must perform a *de novo* review. Thus, despite what the Magistrate Judge recommended, this Court must reconsider the entire matter upon *de novo* review.

Turning to the merits of the staleness argument, numerous courts have recognized that digital files remain on computers for extensive periods of time, even if they have been deleted. As the government correctly notes, forensic experts can often recover deleted computer files. For this reason, many courts have suggested that the staleness issue in the context of digital evidence is somewhat unique, and the passage of time does not necessarily render the evidence stale. *See, e.g. United States v. Payne*, 519 F. Supp.2d 466, 477-78 (D.N.J. 2007) (stating that "the nature of digital evidence [] weighs against a finding of staleness" because computer images are difficult to permanently delete and can often be recovered by forensic experts); *United States v. Wiser-Amos*, 2007 WL 2669377, *2 (W.D. Ky. 2007) ("[G]iven the nature of computer storage, the Court finds it is also reasonable to assume that the computer that originally contained the image in question still contained that image."); *United States v. Toups*, 2007 WL 433562, *4 (M.D. Ala. 2007) ("[I]mages and videos stored on a computer are not easily eliminated from a computer's hard drive. The mere deletion of a particular file does not necessarily mean that the file cannot later be retrieved.").

However, the ability to recover deleted computer files does not, without more, support probable cause to search a residence. There also must be probable cause to

believe that the computer will be located at the residence at the time of the search. Ordinarily, where the time between the downloading of the pornography and the search of the residence is relatively brief, it is easy to infer that the computer is still at the location where the pornography was downloaded. The shorter the time between those two events, the stronger the inference. Conversely, as more time passes between the initial download and the search of the residence, the more attenuated probable cause becomes.

In this case, almost an entire year had elapsed from the time that German authorities initially discovered the child pornography and the time that his residence was searched. During that period, no additional illicit downloads occurred. No new information was discovered, except that agents confirmed that the name on the Verizon account matched the name on the utility records for the residence.² This information confirmed to the agents that the person living at the residence was likely the same person who downloaded the child pornography. However, the defendant correctly points out, nothing about that information confirmed to the agents that computer would still be located at the defendant's address. In fact, the agents had information indicating that the defendant had terminated his internet service, and the agents had no information suggesting that he had simply switched service providers.

Recognizing this deficiency, the government asks this Court to infer, based upon the evidence presented to the Magistrate Judge, the defendant collected or hoarded child pornography. Some courts, including the Second Circuit, have recognized a

² Other than confirming the occupant of the residence, there was no ongoing investigation to explain the delay.

tendency by child pornographers to hoard child pornography. *See, e.g., United States v. Shields*, 458 F.3d 269, 279 n. 7 (3d Cir. 2006)(stating that “collectors of child pornography rarely, if ever, dispose of their collections”); *United States v. Gourde*, 440 F.3d 1065, 1072 (9th Cir. 2006)(finding that the defendant fit the “collector profile” based upon evidence set forth in warrant application); *United States v. Martin*, 426 F.3d 68 (2d Cir. 2005); *Payne*, 519 F. Supp. 2d at 477 (D.N.J. 2007)(taking judicial notice of the fact that individuals who acquire pornography ordinarily retain it for long periods of time). However, in many of those cases, there was evidence from which to infer that the particular defendant collected or hoarded child pornography. For example, in *Martin*, the Second Circuit found probable cause for a search warrant based *inter alia* upon an affidavit that “described the characteristics and proclivities of child-pornography collectors, specifically how they tend to collect such material, store it, and rarely destroy or discard it” and described the defendant’s membership subscription to an illicit e-group. *Martin*, 426 F.3d at 74-75. Similarly, in *Gourde*, the Ninth Circuit found ample cause to infer that the defendant was a hoarder or collector of child pornography based upon his pre-paid unlimited subscription to an illicit website. The Circuit found that this “multi-month” unlimited membership to the website provided agents with “near certainty” that his computer contained evidence of multiple images of child pornography.

In this case, however, was no evidence suggesting that this defendant collected or hoarded child pornography. He did not subscribe to any illicit internet publications or e-groups. He did not have a pre-paid membership. There was no evidence indicating that he had “collected” or downloaded many illicit images. In fact, the search warrant

application referenced only one known image of child pornography having been downloaded from the defendant's computer on one occasion. Under those circumstances, the evidence was insufficient to infer that this defendant collected or hoarded child pornography.

Alternatively, the government asks this Court to assume that the illicit image would still be at the defendant's residence because most people do not replace their computers annually. That is, since it was known that child pornography had been downloaded from an IP address at that residence a year earlier, and since agents had also confirmed that the person using the IP address still lived at the residence, it was proper to assume that the computer onto which the pornography had been downloaded would still be at the residence. Admittedly, this is an exceptionally close case. On the one hand, it is logical to assume that people do not replace their home computers annually. On the other hand, even if it were assumed that most people do not replace their computers annually, the age of the defendant's computer was unknown to the government and the Magistrate Judge at the time the warrant was issued. It was just as likely that defendant Coon had downloaded the image onto a five-year-old computer as it was that he had downloaded it onto a newly-acquired computer. Although this is a very close case, the Court finds that the totality of the circumstances did not support probable cause to issue the warrant. Where, as here, agents were aware of: (1) only one image containing child pornography that (2) had been downloaded almost a full year before the search warrant was issued and (3) no other circumstances to confirm the likelihood that the computer or child pornography would still be at the residence nor (4) evidence from which to infer hoarding of child pornography, the Court finds that

probable cause was lacking.

II. Good Faith Exception

This Court's determination that probable cause was lacking does not necessarily require suppression of the evidence. In *Herring v. United States*, 555 U.S. 135, 129 S.Ct. 695 (2009), the Supreme Court reiterated that the existence of a Fourth Amendment violation does not automatically mandate suppression. Instead, the Court must also consider whether the officers acted "in objectively reasonable reliance" upon the subsequently invalidated search warrant. *Id.* at 701. Where there was "objectively reasonable reliance" (often referred to as "good faith") by the officer, suppression should be denied. Suppression should be the Court's "last resort, not [its] first impulse." *Id.* At 700. In determining whether to grant suppression, courts must balance "the benefits of deterrence" against the social costs of "letting a guilty defendant go free because of the exclusion of possibly probative, but improperly obtained, evidence from use in his prosecution. . . ." See *United States v. Julius*, 610 F.3d 50, 66 (2d Cir. 2010). Accordingly,

[t]o trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system. As laid out in our cases, the exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence.

Herring, 555 U.S. ___, 129 S.Ct. at 702. It is the government's burden to demonstrate that the good faith exception applies. See *United States v. Clark*, ___ F.3d ___, 2011

WL 781597 (2d Cir. March 8, 2011).

A warrant issued by a magistrate judge “normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search.” *Id.*; *United States v. Leon*, 468 U.S. 897, 922 (1984). However, the Second Circuit has identified four situations when the good faith presumption of reasonableness does not apply:

(1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable.

Clark, ___ F.3d at ___, 2011 WL 781597, at *9. (quoting *United States v. Moore*, 968 F.2d 216, 222 (2d Cir. 1992)).

The first scenario does not apply here. There is no indication that Magistrate Judge Scott was knowingly misled. The defendant suggests that this Court can infer an intent to mislead because the agents failed to advise the Magistrate Judge that Coon’s Verizon internet service account had terminated in August 2008. Nothing in the record suggests that the omission was made knowingly with an intent to mislead. Nor was the omission material to the Magistrate Judge’s decision to issue the warrant. In fact, even after learning about the termination of defendant’s Verizon service (in the context of the suppression motion) the Magistrate Judge ultimately reiterated his original determination that there was probable cause to believe the computer containing child pornography would be located at the Coon residence. Because the omission was neither intended to mislead - nor did it mislead - the Magistrate Judge, the first scenario

does not apply.³

As to the second scenario, there has been no claim that the Magistrate Judge wholly abandoned his judicial role in issuing the warrant. Putting aside the third scenario for a moment, the Court finds that the fourth scenario is also inapplicable. The fourth scenario arises when the warrant was so facially deficient that a reasonable officer could not have relied upon it. In *Clark*, the Circuit explained that the fourth scenario applies only when the warrant is so deficient on its face “in failing to particularize the place to be searched or the things to be seized” that the executing officers cannot reasonably presume that it is valid. See *Clark*, ___ F.3d at ___, 2011 WL 781597, at *10. To say that a warrant is facially deficient is not the same thing as saying that the warrant lacks probable cause. The latter reflects a deficiency in the application, whereas the former reflects a deficiency in the actual warrant. *Id.* at *11. Here, the warrant appears to be valid on its face and the defendant has pointed out no flaws.

Finally, the Court turns to the last scenario identified in *Clark* as precluding the application of the good faith exception. This scenario occurs when the warrant application “is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.” *Leon*, 468 U.S. at 923. The Second Circuit has

³ The defendant also takes issue with the agents’ failure to notify the Magistrate Judge that IP address 71.186.130.148 had not been used since April 12, 2008, the date after the child pornography had been downloaded. The date upon which the IP address was last used is wholly irrelevant because, as the defendant concedes, the IP address in this case was likely as “dynamic” IP address which is temporary and can change for any number of reasons. As such, the fact that IP address 71.186.130.148 was never used by the defendant after April 12, 2008 has no bearing on whether the computer remained in the defendant’s home.

explained that this exception “frequently arises when affidavits are bare bones, i.e. totally devoid of factual circumstances to support conclusory allegations” such that the facts indicate that the bare bones description “was almost calculated to mislead.”

Clark, ___ F.3d at ___, 2011 WL 781597, at *12.

Although this Court has found that probable cause to issue the warrant was lacking, the affidavit was not so deficient as to negate an officer’s reasonable reliance upon it. If the application to search had been made shortly after the child pornography was discovered by German authorities, there is little doubt that probable cause would have been found. What negated a probable cause finding was not the absence of evidence, but the passage of time. As more time passed, the likelihood of finding the illegal pornography decreased. However, precisely when probable cause became lacking is a judicial determination upon which reasonable minds can differ. In fact, other district courts have found probable cause in circumstances very similar to the instant case. See, e.g., *United States v. Wiser-Amos*, No. 3:07Cr-42-M, 2007 WL 2669377 (W.D. Ky 2007). Because the warrant application “provided evidence sufficient to create disagreement among thoughtful and competent judges as to the existence of probable cause,” *Leon*, 468 U.S. at 926, the good faith exception applies. See also *United States v. Falso*, 544 F.3d 110, 128 (2d Cir. 2008)(finding that the good faith exception applied when the existence of probable cause was “an issue upon which reasonable minds can differ”). Simply put, the information was not so stale as to negate any objectively reasonable reliance upon the warrant by the officers. See *United States v. Diaz*, 303 F.Supp. 2d 84, 92 (D. Conn. 2004)(“Even if the information

submitted in support of the search warrant was stale or inadequate to constitute probable cause, the good faith exception to the exclusionary rule is applicable to this case.”).

Because the good faith exception applies, the motion to suppress evidence is denied notwithstanding this Court’s determination that probable cause was lacking.

CONCLUSION

In sum, the Court declines to adopt the Second Report and Recommendation. For the reasons set forth herein, the motion to suppress is denied.

SO ORDERED.

s/ Richard J. Arcara

HONORABLE RICHARD J. ARCARA
UNITED STATES DISTRICT JUDGE

DATED: May 16, 2011